

AuditOne Advisory

From Bud Genovese, CEO

The 10 Most Common Mistakes Made Implementing Business Continuity Plans

Mistakes are routinely made when implementing Business Continuity Plans (BCP). After years of comparing regulatory requirements with actual real world implementation data garnered through objective, independent internal auditing and testing, we've compiled a list of the 10 most common mistakes. Below are five of the top ten so we don't overload you this month. We'll share the top five most common BCP mistakes in our next advisory.

10. Security plans during a disaster are missing.

During a disaster, non production systems will typically be used instead of the tested and secure production systems. These temporary systems need to be as secure as the information security program demands. Hackers will not hesitate to attack an institution during a disaster. Make sure the plan takes into consideration physical, logical and administrative security needs during a disaster, just as the FFIEC guidelines recommend.

9. Annual Board Approval is not sought.

Make no mistake, the FFIEC guidelines clearly indicate that the bank's Board of Directors is wholly responsible if response to a disaster is ineffective or impotent. The quality of annual Board oversight and support is a key objective. The most effective BCP processes occur at banks where the Board appoints senior management by name to drive the BCP.

8. Written test plans are missing.

One of the most emphasized objectives in the FFIEC's BCP guidance is the creation of written test plans. Testing is integral to the BCP process and should be performed often (at least annually), cover all critical areas (as discovered during the BIA process), be realistic, and have after-action critiques. Many banks show serious weaknesses in this area, as if the BCP were just an afterthought, and this can cause regulatory criticism.

7. Tests do not take into consideration the loss of key personnel.

Most successful BCP tests occur under ideal conditions, but if you remove a few key personnel, the rubber meets the road and the real lessons are learned. During Hurricane Katrina, circumstances prevented many employees from reporting to assigned locations, despite their best efforts. Don't hope this doesn't happen; plan ahead for it.

6. Procedures are not step by step.

During a disaster, high stress reduces the effectiveness of even the most hardened professionals. The trick is to make things easy on staff. Since key personnel may not be available when needed, create procedures that are very detailed and can be followed by anyone, regardless of the stress.

Give me a call to discuss your Business Continuity Planning or to explore any aspect of your internal audit and risk management program.

Bud Genovese is founder and CEO of AuditOne LLC, a San Jose, California-based internal audit firm that focuses only on banks and their service providers. Mr. Genovese pioneered the concept of providing comprehensive, affordable, independent internal audit services by gathering wide-ranging, world-class expertise within one firm. AuditOne now serves over 100 clients throughout the Western United States, and nationally. Contact Bud Genovese at 408-980-8099 or bud.genovese@audit-one.com